Tweede Kamer der Staten-Generaal 2

Vergaderjaar 2015–2016

29 628 **Politie**

25 124 **Nieuwe infrastructuur mobiele communicatie (C2000)**

Nr. 631 **BRIEF VAN DE MINISTER VAN VEILIGHEID EN JUSTITIE**

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 18 april 2016

Naar aanleiding van de motie van de leden Kooiman en Tellegen (Kamerstuk 29 628, nr. 613) heb ik uw Kamer toegezegd om te bezien of eventuele juridische maatregelen tegen apparaten zoals de Target Blu Eye ondersteunend kunnen zijn aan een doelmatige en ongehinderde uitvoering van de taken van de politie en andere hulpverleningsdiensten. Met deze brief informeer ik u daarover.

In het algemeen overleg «Nationale Veiligheid» van 30 maart jl. heb ik tevens toegezegd om hierbij in breder verband in te gaan op de beveiliging van radionetwerken, zoals C2000, op basis van informatie die hierover in Europees verband is gedeeld.

Detectieapparatuur C2000 – Target Blu Eye

Naar aanleiding van de bovengenoemde motie heeft u mij gevraagd te bezien of eventuele juridische maatregelen tegen apparaten zoals de Target Blu Eye ondersteunend kunnen zijn aan een doelmatige en ongehinderde uitvoering van taken van de politie en andere hulpverleningsdiensten. Vooralsnog ben ik van mening dat een verbod nuttig kan zijn en ben ik bereid om over te gaan tot een verbodsbepaling als de noodzaak hiervan voldoende onderbouwd kan worden. Hiertoe zal ik de komende maanden nader onderzoek laten uitvoeren. Hieronder zal ik mijn reactie toelichten.

Vrije marktwerking

Voor een eventuele verbodsbepaling op apparaten is van belang dat vanuit vrije marktwerking het Europees, maar ook nationaal, niet zonder meer mogelijk is om apparaten die op de markt zijn te verbieden. Een verbod op het bezit en verhandelen van dergelijke apparaten kan worden aangemerkt als een maatregel die het vrij verkeer van goederen

kst-29628-631
ISSN 0921 - 7371
’s-Gravenhage 2016

belemmert. Dat is, in de gegeven situatie, alleen toelaatbaar te achten wanneer het unierecht daar uitdrukkelijk ruimte toe laat. Hiervan zou sprake kunnen zijn indien de maatregel nodig zou zijn ter bescherming van, voor zover hier van belang, de openbare orde of de openbare veiligheid. Daarnaast zou nog een rechtvaardigingsgrond kunnen bestaan indien de belemmering nodig is in verband met een zwaarwegend maatschappelijk belang. Daarbij moet dan aangetoond kunnen worden dat die maatregel geschikt en noodzakelijk is om het ingeroepen belang te beschermen.

In alle gevallen zal feitelijk aangetoond moeten kunnen worden niet alleen dat het gebruik van de apparaten leidt tot een inbreuk op bijvoorbeeld het belang van opsporing van strafbare feiten of rechtshandhaving, maar ook dat een verbod een daadwerkelijke verbetering zou teweegbrengen, alsmede dat er geen minder zwaarwegende alternatieven voorhanden zijn. Zoals ik u ook in mijn vorige brief hierover aangaf, houdt de politie er in haar werkwijze rekening mee dat deze apparatuur door derden kan worden gebruikt. Op deze manier kunnen potentiële negatieve effecten van het gebruik worden beperkt.

Vergelijking andere verboden

Bij mijn nadere overweging of en zo ja, welke juridische maatregelen tegen apparaten als de Target Blu Eye zouden kunnen worden getroffen, heb ik ook vergelijkbare maatregelen betrokken, zoals het verbod op de apparatuur voor snelheidsradardetectie en het verbod op inbrekerswerktuigen. In het geval van het verbod op apparatuur voor snelheidsradardetectie heeft het radarontvangstapparaat enkel en alleen tot doel te voorkomen dat een overschrijding van de maximumsnelheid wordt opgemerkt. Bovendien kan het gebruik van de radardetector de verkeersveiligheid in gevaar brengen. Zoals u weet wordt de Target Blu Eye in de markt gezet met het primaire gebruiksdoel om radiosignalen van hulpdiensten op te pikken zodat een bestuurder hiernaar kan handelen, door bijvoorbeeld eerder op zij te gaan, als een van de hulpdiensten met spoed wil passeren. Het enkele bezit of gebruik van de Target Blu Eye veroorzaakt hierbij in beginsel geen schade of onveilige situatie. Dat wordt anders als dit voorwerp aantoonbaar wordt gebruikt als hulpmiddel om een strafbaar feit te plegen. In dat geval zijn inbeslagneming en verbeurdverklaring mogelijk als ondersteunende juridische maatregelen om tegen dat gebruik op te treden.

Bij een verbod op inbrekerswerktuigen, zoals dat in veel gemeentelijke APV's is opgenomen, is het voorhanden hebben of vervoeren van lopers, valse sleutels, touwladders etc. strafbaar gesteld, soms alleen tijdens de nachtelijke uren. Het verbod geldt niet als de inbrekerswerktuigen niet zijn gebruikt of bestemd voor het vergemakkelijken van een inbraak of het wissen van sporen. Een vergelijkbaar verbod voor de Target Blu Eye heeft als belangrijk bezwaar dat bij het aantreffen van dit voorwerp enige relatie met een (voorgenomen) strafbaar feit niet uit zijn uiterlijke verschijningsvorm valt af te leiden. Dit klemt temeer omdat het voorwerp vooralsnog ook een legaal gebruiksdoel heeft. Verwacht mag worden dat een bezitter te kwader trouw uiteraard geen helderheid zal verschaffen over zijn bedoelingen met het voorwerp. Pas als ook andere feiten en omstandigheden duiden op criminele intenties en activiteiten is voorstelbaar dat aannemelijk kan worden gemaakt dat daarbij de Target Blu Eye als hulpmiddel is gebruikt. Zoals hiervoor is aangegeven, zijn in dat geval inbeslagneming en verbeurdverklaring de geschikte instrumenten om het voorwerp uit het verkeer te nemen.

Conclusie

De politie heeft op basis van een eerste inventarisatie in reactie op de media-aandacht aangegeven het gebruik van de Target Blu Eye niet als structureel probleem te ervaren. Op basis van enkele voorbeelden geeft de politie evenwel ook aan dat het gebruik van de Target Blu Eye in potentie hinderlijk kan zijn voor de opsporing. Daarom houdt de politie in haar werkwijze ook al rekening met het gebruik van dergelijke apparatuur. Een verbodsbepaling zou hierop een nuttige aanvulling kunnen zijn. Gelet op de regels van vrije marktwerking is voor een eventuele verbodsbepaling een aantoonbare noodzaak voorwaardelijk. Ik ben bereid om over te gaan tot een verbodsbepaling als de noodzaak hiervan voldoende onderbouwd kan worden. Hiertoe zal ik de komende maanden nader onderzoek laten uitvoeren. Op basis van de resultaten van dit onderzoek zal ik u berichten over eventuele vervolgstappen.

Beveiliging van radiocommunicatie via de zogenaamde TETRA-standaard

In oktober 2015 heeft een Zweedse politiebond een presentatie gegeven over de beveiliging van radiocommunicatie via de zogenaamde TETRA-standaard. Zoals GSM de standaard is voor mobiele telefonie voor het grote publiek, is TETRA de standaard voor mobiele communicatie voor de Openbare Orde en Veiligheidsdiensten en wordt deze ook gebruikt voor andere kritische communicatieprocessen in het bedrijfsleven. Deze presentatie is in Europees verband verspreid en heeft mijn departement op 8 maart jl. ontvangen.

De presentatie stelt dat aangenomen mag worden dat de radiocommunicatie welke verloopt via radionetwerken die gebruik maken van de wereldwijde TETRA-standaard afgeluisterd kan worden door buitenlandse inlichtingendiensten.
Net als overigens in ca. 147 andere landen maken de Nederlandse hulpverleningsdiensten voor hun radiocommunicatie met C2000 gebruik van deze technologie. Tevens wordt gesteld dat bedrijven apparatuur en software op de markt aanbieden om TETRA-systemen te «scannen» en te «monitoren».

Met betrokkenheid van het Nationaal Bureau voor Verbindingsbeveiliging (NBV), businessunit van de AIVD, het NCSC en de politie is de informatie uit de presentatie beoordeeld en afgezet tegen de eerdere veiligheidsinschattingen die voor C2000 zijn gemaakt en de maatregelen die zijn genomen om de communicatie via C2000 te beveiligen. Ik hecht eraan u hierover te informeren.

Beveiligingsniveau C2000

C2000 is het communicatiesysteem voor de reguliere communicatie tussen de hulpverleningsdiensten: politie, brandweer, ambulance en Koninklijke Marechaussee. Het beveiligingsniveau voor deze gebruikersgroepen is bepaald op het niveau van «departementaal vertrouwelijk». Dit betekent dat het systeem zonder aanvullende maatregelen niet bedoeld is voor communicatie boven dit niveau. Gebruikersgroepen van C2000 met hogere beveiligingseisen kunnen gebruik maken van extra beveiligingsmaatregelen, waaronder extra versleuteling van het berichtenverkeer.

Het C2000-netwerk wordt beveiligd door een combinatie van fysieke (hekken, sloten), organisatorische (screening personeel) en elektronische (alarmering, versleuteling van de radiocommunicatie) beveiligingsmaatregelen. Als bijvoorbeeld een portofoon als vermist/gestolen wordt

gedetecteerd en dit wordt gemeld, dan wordt deze geblokkeerd. Dit kan een tijdelijke of een permanente blokkering opleveren, waardoor deze randapparatuur onbruikbaar is geworden voor onbevoegden.

Interceptiemogelijkheden door statelijke actoren en niet statelijke actoren

De hierboven genoemde TETRA-standaard wordt wereldwijd ook buiten de overheid gebruikt voor radiosystemen voor de zakelijke telecommarkt (o.a. ten behoeve van het mobilofoonverkeer van het openbaar vervoer, industrie, logistiek en bewaking). Deze systemen kennen in veel landen de wettelijke plicht om interceptiemogelijkheden te hebben: afluisterbaar te zijn. Met andere woorden, de mogelijkheid voor aftappen binnen wettelijke kaders is niet nieuw.

In de presentatie wordt ook de mogelijkheid van interceptie via een zogenaamde verborgen «achterdeur» aan de orde gesteld. Zowel politie als AIVD geeft in reactie op deze informatie aan vanuit haar informatielijn nooit een «achterdeur» te hebben aangetroffen of aanwijzingen dat hiervan gebruik wordt gemaakt vernomen. Zij geven aan, dat daar waar gesuggereerd wordt dat er moedwillig in de apparatuur zaken worden ingebouwd om de communicatiesystemen te kunnen afluisteren dit, hoewel theoretisch niet uit te sluiten, vooralsnog niet gestaafd is door bewijs of concrete vermoedens.

Het radioverkeer van C2000 wordt beveiligd met twee lagen versleuteling. Dit zijn de standaard aanwezige C2000 versleuteling voor alle gebruikersgroepen en aanvullende versleuteling voor specifieke gebruikersgroepen. Zowel de politie als de AIVD hebben ook ten aanzien van niet-statelijke actoren (civiele beveiligingsonderzoekers, criminele organisaties, activisten, terreurgroepen etc.) geen aanwijzingen dat deze actoren proberen om de standaard versleuteling van C2000 te doorbreken. Hoewel de AIVD geen diepgaand onderzoek heeft verricht naar het gebruikte crypto-algoritme, kan ten aanzien van de aanvullende versleuteling gesteld worden dat dit geavanceerde beveiliging biedt tegen het illegaal meeluisteren door derden.

Tenslotte wordt er in de presentatie gesteld dat bedrijven apparatuur en software op de markt aanbieden om TETRA-systemen te «scannen» en te «monitoren». De genoemde bedrijven variëren van bedrijven die zelf TETRA systemen produceren tot bedrijven die scan-, encryptie- en decryptie-apparatuur leveren. Het scannen en monitoren van standaard TETRA zonder een beveiligingsalgoritme behoort tot de mogelijkheden van deze bedrijven. Dit is een legale activiteit en kan voor allerlei doeleinden worden gebruikt, bijvoorbeeld om de netwerkkwaliteit te meten. C2000 is beveiligd met een «versleutelings-algoritme» dat niet toegankelijk is voor deze bedrijven en waarvan het illegaal ontsleutelen ook niet door deze bedrijven wordt aangeboden. De politie heeft mij daarbij aangegeven tot op heden geen apparatuur aangetroffen te hebben die de inhoud van C2000 Tetra kan ontcijferen. Het detecteren van het radiosignaal is wel mogelijk, zoals in het eerste deel van de brief aangegeven.

Het beveiligen van informatie en communicatie tussen hulpverleningsdiensten vindt zoals hierboven vermeld plaats op basis van een combinatie van fysieke, personele en technische maatregelen. Vooralsnog zie ik op basis van de presentatie en de hierover ontvangen informatie van de AIVD, het National Cyber Security Centre en de politie geen aanleiding om de huidige beveiligingsmaatregelen te veranderen.

De presentatie is voor mij wel aanleiding om signalen over de beveiliging van Tetra in nationaal en internationaal verband nader te verkennen en indien nodig van aanvullend onderzoek en of maatregelen te voorzien. Daarbij is het van belang ons te realiseren dat ontwikkelingen in technologieën, inclusief de kwetsbaarheden daarin, steeds zullen voortgaan en wij hier altijd scherp en bedacht op moeten blijven.

De Minister van Veiligheid en Justitie,
G.A. van der Steur